REMARKS

Claims 1-35 were pending. All stand rejected. The applicants have amended claims 1, 2, 12, 15-17, 19-21, 25, 28, 29, 32 and 35, cancelled claim 34 and added new claims 36-39. Therefore, claims 1-33 and 35-39 are presently pending. The applicants request further consideration and re-examination in view of the amendments above and remarks set forth below.

The applicants amended the specification to correct an informality at page 11, line 10.

Rejections under 35 U.S.C. § 102:

Claims 1-5, 7-9, 13-15, 17, 18, 20, 23, 24 and 28-34 are rejected as under 35 U.S.C. § 102 as being anticipated by U.S. Patent Publication No. 2002/0194484 to William J. Bolosky et al. (hereinafter "Bolosky et al.").

As amended, claim 1 recites a method of file access control comprising: storing an encrypted filename of a file at a location in a computing system; converting the encrypted filename into a plaintext filename; modifying the plaintext filename into a modified filename; and authorizing an entity to access the file for performing a write operation on the file by comparing the modified filename to the stored encrypted filename.

Bolosky et al. disclose a distributed file system in which a writer of a file can provide file authentication information to a verifying machine without having to compute a new digital signature every time a file is written. Bolosky et al., Abstract. This is accomplished by the writer periodically compiling a list of the hash values of all files that have been written over a recent interval, computing a hash of the list and signing the hash (the list is referred to by Bolosky et al. as a "manifest, akin to a shipping manifest that enumerates the items of the shipment"). Bolosky et al., Abstract.

The examiner relies on Bolosky et al. at paragraphs [0033], [0034], [0119], [0156], and [0160] in rejecting original claim 1. In paragraphs [0033] and [0034], Bolosky et al. explains that in its distributed file system, contents of files and directory entries are encrypted and only authorized users are given the decryption key. In paragraph [0119], Bolosky et al. explain that to grant access to multiple users, the file system maintains a user key list for each file. In paragraph [0156], Bolosky et al. explain that to read a target block of a file, a control module 220 calls on a

cryptographic engine 224 to decrypt the target block using a symmetric cipher and a recovered hash value as the key. In paragraph [0160], Bolosky et al. explain that when a file is modified, a new hash value is computed because the previous computed hash value is rendered unusable, the new hash value is used to encrypt the block and the new encrypted block replaces the previous block.

In paragraph [0037], Bolosky et al. state that read access control entries are created for each authorized user who is granted read access to an encrypted file. In this same paragraph, Bolosky et al. further states that:

> Write access control is governed by the directory server that stores the directory entry for the file, and it is thus not addressed by the file format and is not discussed further within this document. All references to "access" within this document refer to read access.

(Emphasis added). Thus, Bolosky et al. refers only to the grant of read access to a file. As stated in paragraph [0037], Bolosky et al. do not discuss granting write access. In contrast, amended claim 1 recites authorizing an entity to access a file for performing a write operation on the file. For at least this reason, claim 1 is allowable over Bolosky et al.

Moreover, claim 1 recites a specific sequence of steps which are performed in connection with the authorization to perform a write operation. Specifically, claim 1 requires storing an encrypted filename of a file at a location in a computing system; converting the encrypted filename into a plaintext filename; modifying the plaintext filename into a modified filename; and authorizing an entity to access the file for performing a write operation on the file by comparing the modified filename to the stored encrypted filename. Bolosky et al. do not suggest or disclose these steps which are performed in connection with authorizing an entity to access a file for performing a write operation on the file n. For example, paragraphs [0156] and [0160] of Bolosky et al., which are relied upon by the examiner in rejection claim 1, discuss decryption and encryption of the contents of a file. These paragraphs have nothing to do with the grant of write access to the file, but instead, refer to processing of file contents after the file has been accessed. This is another reason why claim 1 is allowable over Bolosky et al.

Still further, claim 1 requires storing an encrypted filename, decrypting the filename, modifying the filename and using the modified filename for comparison for

authorizing access to the file. Bolosky et al. explain in paragraphs [0118]-[0126] how its key list is used for controlling access to a file. According to Bolosky et al., this is accomplished by providing a list of user names and keys for the users. Figure 7 of Bolosky et al. Bolosky et al. do not suggest or disclose using a modified filename for comparison in order to authorize access to the file. This is yet another reason why claim 1 is allowable over Bolosky et al.

Claims 2-5, 7-9, 13-14 are dependent from claim 1. Therefore, these claims are allowable over Bolosky et al. for at least the same reasons claim 1 is allowable. Moreover, these claims recite limitations not suggested or disclosed by Bolosky et al. For example, claim 2, as amended, recites using a key that comprises a combination of two encryption keys to convert the encrypted filename into the plaintext filename. Bolosky et al. do not disclose such a feature. Paragraphs [0154]-[0156] of Bolosky et al., which were relied upon by the examiner in rejecting claim 2, discuss extraction of keys. However, this portion of Bolosky et al. do not suggest or disclose the use of a key that is combination of two keys to convert an encrypted filename into a plaintext filename. This is another reason why claim 2 is allowable over Bolosky et al.

As another example, claim 3 recites using a first one of the two encryption keys to encrypt the plaintext filename into the modified filename. Paragraph [0119] of Bolosky et al., which was relied upon by the examiner in rejecting claim 3, discusses the use of a key list. This portion of Bolosky et al. do not suggest or disclose the unique features of claim 3 in which a combination key, which is a combination of two keys, is used for one purpose and one of the keys of the combination key is used for another purpose. This is another reason why claim 3 is allowable over Bolosky et al.

As yet another example, claim 4 recites using the second one of the two encryption keys to encrypt the modified filename to form a result and determining whether the result matches the encrypted filename. The examiner relies on Paragraphs [0154]-[0156] of Bolosky et al. as disclosing the features of claim 4. However, this portion of Bolosky et al. does not suggest or disclose the unique features of claim 4 in which a combination key is used for one purpose and another one of the keys of the combination key is used for a different purpose. This is another reason why claim 4 is allowable over Bolosky et al.

As still another example, claim 5 recites using a first one of the two encryption keys to encrypt the plaintext filename and performing a hash function on

the filename thereby forming the modified filename. Paragraph [0037] of Bolosky et al., which was relied upon by the examiner in rejecting claim 5, discusses the use of read access control keys. This portion of Bolosky et al. does not suggest or disclose the features of claim 5 in which a combination key is used for one purpose and one of the keys of the combination key is used for another purpose. This is another reason why claim 5 is allowable over Bolosky et al.

Claim 15, as amended, recites an apparatus for controlling access to a file, comprising: a server for the storing an encrypted filename associated with a file; and a client in communication with the server for retrieving the encrypted filename from the server, for converting the encrypted filename into a plaintext filename and for modifying the plaintext filename into a modified filename, wherein the client provides the modified filename to the server and wherein the server determines whether the client is authorized to perform a write operation on the file by comparing the modified filename received from the client to the stored encrypted filename.

Thus, claim 15 recites that a server makes a determination of whether a client is authorized to perform a write operation. As explained above, Bolosky et al. state in paragraph [0037] that they do not discuss granting write access. For at least this reason, claim 15 is allowable over Bolosky et al.

Moreover, claim 15 recites specific features in connection with the determination of whether a client is authorized to perform a write operation. Specifically, claim 15 recites that the server stores an encrypted filename, the client retrieves the encrypted filename from the server, converts the encrypted filename into a plaintext filename and modifies the plaintext filename into a modified filename. The client provides the modified filename to the server and the server determines whether the client is authorized to perform a write operation on the file by comparing the modified filename received from the client to the stored encrypted filename. Bolosky et al. do not suggest or disclose these features. For example, paragraphs [0156] and [0160] of Bolosky et al., which are relied upon by the examiner in rejecting claim 15, discuss decryption and encryption of the contents of a file. These paragraphs have nothing to do with the grant of write access to the file, but instead, refer to the processing of file contents after the file has been accessed. This is another reason why claim 15 is allowable over Bolosky et al.

Still further, claim 15 requires storing an encrypted filename, decrypting the filename, modifying the filename and using the modified filename for comparison for

determining whether the client is authorized access to the file. As explained above, Bolosky et al. do not suggest or disclose using a modified filename for comparison in order to control access to the file. This is yet another reason why claim 15 is allowable over Bolosky et al.

Claims 17, 18, 20, 23, 24 are dependent from claim 15. Therefore, these claims are allowable over Bolosky et al. for at least the same reasons claim 15 is allowable. Moreover, similarly to claims dependent from claim 1 as explained above, these claims recite limitations not suggested or disclosed by Bolosky et al. For example, claim 17 recites that the client converts the encrypted filename into the plaintext filename using a key that comprises a combination of two encryption keys. Paragraphs [0154]-[0156] of Bolosky et al., which were relied upon by the examiner in rejecting claim 17, discuss extraction of keys. However, this portion of Bolosky et al. does not suggest or disclose the use of a key that is combination of two keys to convert an encrypted filename into a plaintext filename. This is another reason why claim 17 is allowable over Bolosky et al.

As another example, claims 18 and 20 recite that the client forms the modified filename using a first one of the two encryption keys to encrypt the plaintext filename. Paragraph [0119] of Bolosky et al., which was relied upon by the examiner in rejecting claims 18 and 20, discusses the use of a key list. This portion of Bolosky et al. does not suggest or disclose the unique features of claims 18 and 20 in which a combination key, which is a combination of two keys, is used for one purpose and one of the keys of the combination key is used for another purpose. This is another reason why claims 18 and 20 are allowable over Bolosky et al.

As amended, claim 28 recites an apparatus for controlling access to a file comprising a server having a stored encrypted filename of a file, the server being in communication with a writer and a reader, the writer being a client of the server and having a first key that permits the writer to write to the file and the reader being another client of the server and having a combination key that comprises a combination of the first key and a second key wherein the combination key permits the reader to read the file.

Bolosky et al. do not suggest or disclose all of the features of claim 28. For example, claim 28 recites a first key that permits the writer to write to the file and a combination key that comprises a combination of the first key and a second key wherein the combination key permits the reader to read the file. However, paragraph

[0119] of Bolosky et al., which was relied upon by the examiner in rejecting claim 28, explains that to grant access to multiple users, the file system maintains a user key list for each file. As explained above, Bolosky et al. state in paragraph [0037] that they do not discuss granting write access. Moreover, Bolosky et al. do not teach or suggest that a combination key, which is a combination of two keys, is used for one purpose and one of the keys of the combination key is used for another purpose. For at least these reasons, claim 28 is allowable over Bolosky et al.

Claims 29-31 are allowable at least because they are dependent from an allowable base claim 28. Moreover, claims 29-31 recite limitations not suggested or disclosed by Bolosky et al. For example, claim 29 recites that the stored encrypted filename is obtained by encrypting a filename of the file using the combination key. Paragraph [0119] of Bolosky et al., which was relied upon by the examiner in rejecting claim 29, discusses the use of a key list. This portion of Bolosky et al. does not suggest or disclose the unique features of claim 29 in which a combination key, which is a combination of two keys, is used for encrypting a filename of the file. This is another reason why claim 29 is allowable over Bolosky et al.

Claim 30 recites that the server determines that the writer is authorized to write to the file by receiving from the writer the filename encrypted using the first key, encrypting the received filename again using the second key thereby forming a twice encrypted filename and comparing the twice encrypted filename to the stored encrypted filename. Claim 31 recites that the server determines that the writer is authorized to write to the file by receiving from the writer the filename encrypted using the first key, applying a hash function to the received filename thereby forming a computed hash value and comparing the computed hash value to a stored hash value. Paragraphs [0119]-[0126] of Bolosky et al., which were relied upon by the examiner in rejecting claims 30 and 31, discuss the use of a key list. Paragraphs [0127] and [0128] of Bolosky et al., which were also relied upon by the examiner in rejecting claims 30 and 31, discuss verifying authenticity of a file. Paragraphs [0129] and [0130] of Bolosky et al., which were also relied upon by the examiner in rejecting claims 30 an d 31, discuss making updates to the contents of a file. Bolosky et al. do not suggest or disclose the unique features of claim 30 or claim 31. This is another reason why claims 30 and 31 are allowable over Bolosky et al.

As amended, claim 32 recites an apparatus for controlling access to a file comprising a server having a first stored encrypted filename of the file and a second

stored encrypted filename of the file, the server being in communication with a writer and a reader, the writer being a client of the server and having a first key that permits the writer to write to the file and the server determining whether the writer is authorized to write to the file by receiving from the writer the filename encrypted using the second key and comparing the received filename to the second stored encrypted filename and the reader being another client of the server and having a second key that permits the reader to read the file.

Bolosky et al. do not suggest or disclose all of the features of claim 32. For example, claim 32 requires determining whether the writer is authorized to write to the file by receiving from the writer the filename encrypted using the second key and comparing the received filename to the second stored encrypted filename. However, paragraph [0119] of Bolosky et al., which was relied upon by the examiner in rejecting claim 32, explains that to grant access to multiple users, the file system maintains a user key list for each file. And as explained above, Bolosky et al. state in paragraph [0037] that they do not discuss granting write access. Moreover, Bolosky et al. do not teach or suggest the use of comparing a received encrypted filename to a stored encrypted filename in order to control access to a file. For at least these reasons, claim 32 is allowable over Bolosky et al. Claims 33 and 35 are allowable at least because they are dependent from an allowable base claim 28.

Rejections under 35 U.S.C. § 103:

Claims 6, 10, 11, 19, 21, 22, 25-27 and 35 are rejected under 35 U.S.C. § 103 as being unpatentable over Bolosky et al. in view of U.S. Patent No. 6,847,995 to Edward A. Hubbard (hereinafter "Hubbard").

The rejection of claims 6, 10 and 11 relies on the premise that Bolosky et al. disclose all of the limitations of claim 1. However, as explained above, Bolosky et al. do not disclose all of the limitations of claim 1. Hubbard does not appear to disclose these limitations either. Accordingly, at least because they are dependent from an allowable base claim 1, claims 6, 10 and 11 are allowable over Bolosky et al. and Hubbard.

The rejection of claims 19, 21, 22, 25-27 relies on the premise that Bolosky et al. disclose all of the limitations of claim 15. However, as explained above, Bolosky et al. do not disclose all of the limitations of claim 15. Hubbard does not appear to disclose these limitations either. Accordingly, at least because they are dependent

from an allowable base claim 15, claims 19, 21, 22, 25-27 are allowable over Bolosky et al. and Hubbard.

The rejection of claim 35 relies on the premise that Bolosky et al. disclose all of the limitations of claim 32. However, as explained above, Bolosky et al. do not disclose all of the limitations of claim 32. Hubbard does not appear to disclose these limitations either. Accordingly, at least because it is dependent from an allowable base claim 32, claim 35 is allowable over Bolosky et al. and Hubbard.

Claims 12 and 16 are rejected under 35 U.S.C. § 103 as being unpatentable over Bolosky et al. in view of U.S. Publication No. 2002/0062451 to Edward M. Scheidt et al. (hereinafter "Scheidt et al.")

The rejection of claims 12 and 16 relies on the premise that Bolosky et al. disclose all of the limitations of claims 1 and 15. However, as explained above, Bolosky et al. do not disclose all of the limitations of claims 1 and 15. Scheidt et al. do not appear to disclose these limitations either. Accordingly, at least because they are dependent from an allowable base claim 1 or 15, claims 12-16 are allowable over Bolosky et al. and Scheidt et al.

New claims 36-39:

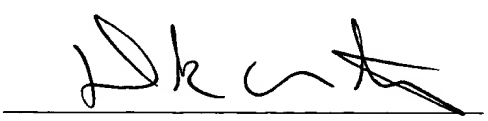
New claims 36-39 are dependent from an allowable base claim 1 or 15. For at least this reason, claims 36-39 are allowable. New claims 36-39 are supported by the applicants' specification at least at page 8, lines 15-31.

Conclusion:

In view of the above, the applicants submit that all of the pending claims are now allowable. Allowance at an early date would be greatly appreciated. Should any outstanding issues remain, the examiner is encouraged to contact the undersigned at (408) 293-9000 so that any such issues can be expeditiously resolved.

Respectfully Submitted,

Dated: Aug. 12, 2005



Derek J. Westberg (Reg. No. 40,872)